Advanced Encryption Standard in Counter Mode

Sai Kyaw Thuya, Khin Than Mya

University of Computer Studies, Yangon

Sniper173@gmail.com

Abstract

As the information technology communication advances, there is a need for strong interest in the information security. Encryption is one of the alternative techniques that can be applied to any system for safeguarding sensitive data. The National Institute of Standards and Technology (NIST) recently selected the Advanced Encryption Standard (AES) . also known as Rijndael. The AES is a block cipher , and it can be used in many different modes. AES itself is a very strong cipher, and counter mode makes it difficult for an eaveasdropper to sport patterns. This system implements the use of AES Counter Mode (AES-CTR), with an explicit initialization vector (IV). We will apply Linear Congruential Method (LCM) for IV generation and a decentralized approach for key distribution. AES-CTR has many properties that make it an attractive encryption algorithm for in high-speed networking.